A Draft Framework for Designing Cryptographic Key Management Systems (DSP 800-130)

Elaine Barker
Dennis Branstad
Santosh Chokhani
Miles Smid (Presenter)

NIST Key Management Workshop
September 10, 2012

Purpose of Presentation

- To provide a brief history of the Framework
- To review what we mean by a Framework for Cryptographic Key Management
- To explain how the Framework supports the NIST Federal Cryptographic Key Management System Profile
- To present the main concepts and provisions of the draft
- To obtain final comments before publication

History of SP 800-130 Development

- First NIST Key Management Workshop (June 8-9 2009)
  - Essentials of a Cryptographic Key Management Framework
- First Public Comment Draft (June 15, 2010)

History Continued

- Second NIST Key Management Workshop (September 20-21, 2010)
  - Comments from seven organizations presented and discussed
- Second Public Comment Draft (April 2012)
- Third NIST Key Management Workshop (September 10-11, 2012)

What is a CKMS?

- A CKMS consists of policies, procedures, components and devices that are used to protect manage and distribute cryptographic keys and certain specific information, called (associated) metadata.
- A CKMS includes any device or sub-system that can access an unencrypted key or its metadata.

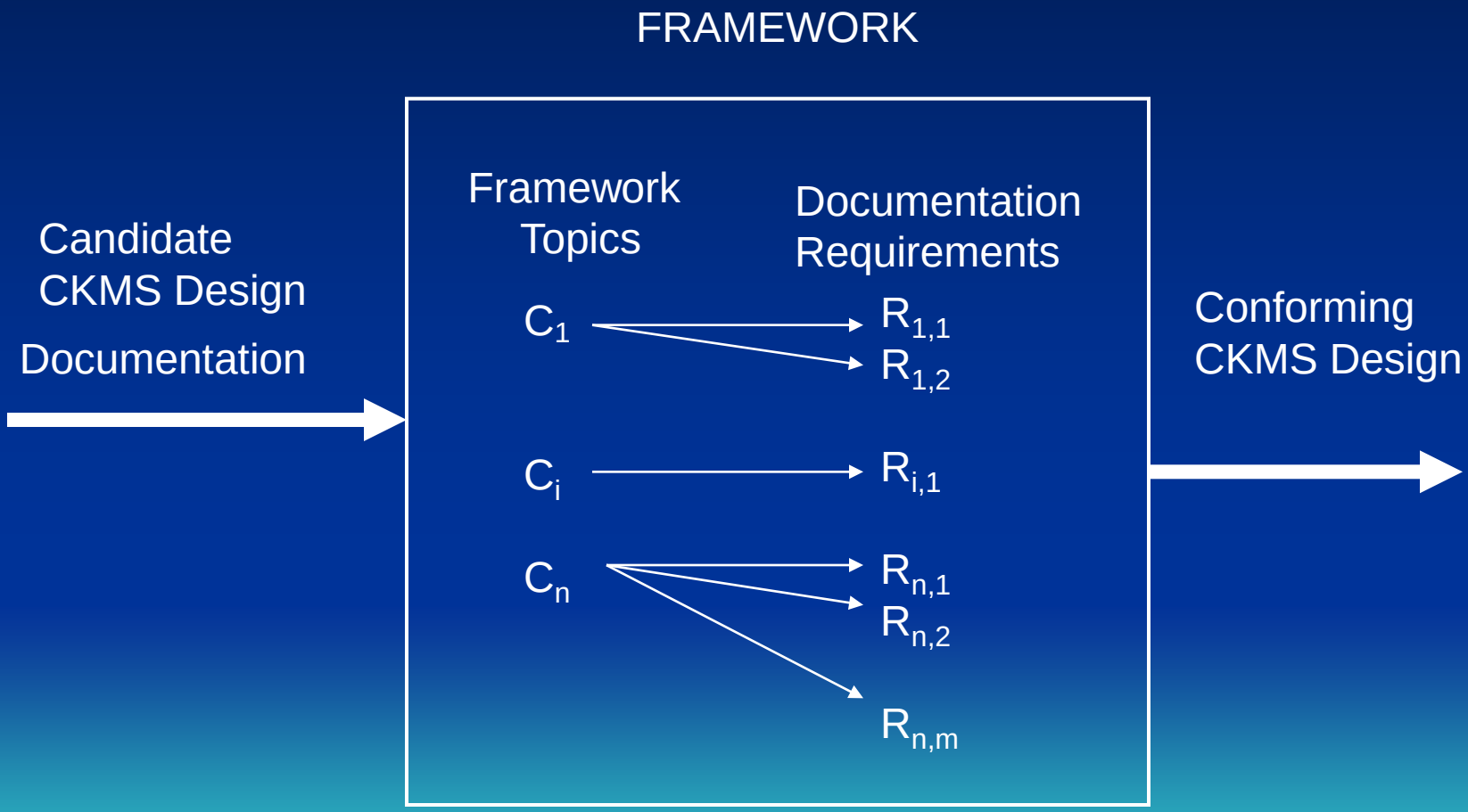
If you were to buy, implement, or use a CKMS, what would you like to know?

- Its Cost
- Its Features and Capabilities
  - What does it do?
  - How does it do it?
  - What is protected?
  - How is the protection provided?
  - How is it used?
- How secure is it?

What is a CKMS Framework?

- A CKMS Framework provides design documentation requirements
- A Framework is an organized list of Framework topics and individual CKMS design documentation requirements.
- The Framework asks for a complete uniform specification of the CKMS

Framework Topics and Design Documentation Requirements



Scope and Construction

- The CKMS provides key management and/or metadata protection functions such as generation, distribution, storage, use, revocation, and destruction of cryptographic keys and metadata.
- The CKMS supports but does not include applications.
- The Framework places requirements on the CKMS design documentation by using the word “shall”.
- The Framework is not judgmental.

Framework Advantages

- Encourages CKMS designers to consider the factors needed in a comprehensive CKMS
- Encourages CKMS designers to consider factors that if properly addressed will improve security
- Helps define the CKMS design task by requiring the specification of significant CKMS capabilities
- Assists in logically comparing different CKMS and their capabilities
- Improves security by specifying what capabilities are implemented and supported
- Forms the basis for a U.S. Federal CKMS Profile

Framework Limitations

- Does not require specific CKMS capabilities or design choices
- Does not guarantee “security”
- Does not mandate protections for U.S. Government sensitive information
- Any CKMS if properly specified should be able to comply with the Framework, but not all CKMS will comply with the U.S. Government CKMS Profile

What is a CKMS Profile?

- A CKMS Profile provides the requirements that a qualifying CKMS, its implementation and its operation must meet.
- A CKMS Profile specifies how the CKMS must be designed, implemented, tested, and operated.
- A CKMS Profile is limited to a particular group or area of interest (e.g. US Government and Government contractors)

CKMS Framework Topics

1. Introduction
2. Framework Basics
3. Goals
4. Security Policies
5. Roles and Responsibilities
6. Cryptographic Keys and Metadata
7. Interoperability and Transitioning
8. Security Controls
9. Testing and System Assurances
10. Disaster Recovery
11. Security Assessment
12. Technical Challenges

1. Introduction

- A conformant CKMS design **shall** meet (address/document) all "**shall**" requirements of the Framework.

1.1 Scope of Framework

1.2 Audience

1.3 Organization

2. Framework Basics

2.1 Rationale for Cryptographic KM

2.2 Keys, Metadata, Trusted Associations, and Bindings

2.3 CKMS Applications

2.4 Framework Topics and Requirements

2.5 CKMS Design

2.6 Example CKMS supporting E-Mail

2.7 Components and Devices

2.1 Rationale for Cryptographic KM

- Specify all cryptographic algorithms and supported key sizes
- Specify the estimated security strength (bits of security) of cryptographic mechanisms

2.4 Framework of Topics and Requirements

- The CKMS design **shall** make selections and provide documentation as required by the requirements of the Framework

2.7 CKMS Components and Devices

- Specify (e.g., make, model, and version) all major devices

3. Goals

3.1 KM for Networks, Applications, and Users

3.2 Conformance to Standards

3.3 Ease-of-Use

3.4 Performance and Scalability

3.5 Maximize Use of COTS products

3.1 KM for Networks, Applications, and Users

- Specify the goals of the CKMS with respect to the communications networks on which it will function
- Specify the applications that the CKMS intended to support
- Specify the intended number of users and responsibilities placed on the users

3.2 Conformance to Standards

- Specify the Federal, national, and international standards that are utilized by the CKMS and how is conformance tested for each
- Specify what commercial products are utilized in the CKMS design
- Specify the security standards to which the CKMS conforms

3.3 Ease of Use

- Specify the user interfaces and their design principles
- Specify the results of the user acceptance tests
- Specify human error prevention or failsafe features are designed into the system

3.4 Performance and Scalability

- Specify the performance characteristics of the CKMS (e.g., average and peak workloads and response times)
- Specify the extent that the CKMS can be scaled to exceed the peak performance characteristics if necessary

3.5 Maximize Use of COTS Products

- Specify the COTS products used in the CKMS design
- Specify which security functions are performed by COTS products
- Specify how COTS products are configured and augmented to meet the goals of the CKMS

4. Security Policies

4.1 Information Management Policy

4.2 Information Security Policy

4.3 CKMS Security Policy

4.4 Other Related Security Policies

4.5 Interrelationships among Policies

4.6 Accountability

4.7 Anonymity, Unlinkability, and Unobservability

4.8 Laws, Rules, and Regulations

4.9 Security Domains

4.3 CKMS Security Policy

- Specify the CKMS Security Policy that is enforced.
- Specify how the CKMS Security Policy is enforced
- Specify how any automated portions of the CKMS Security Policy are expressed (e.g., in tabular form or formal language) such that the CKMS can enforce them

4.4 Other Related Security Policies

- Specify other related security policies that support the CKMS Security Policy

4.5 Interrelationships among Policies

- Specify the policies that describe the conditions under which keys and their metadata may be shared

4.6 Accountability

- Specify how accountability is enforced by the CKMS

4.7 Anonymity, Unlinkability, and Unobservability

- Specify anonymity unlinkability, and unobservability policies supported by CKMS
- Specify how these features are achieved

4.8 Laws, Rules, and Regulations

- Specify countries where CKMS is intended for use and any legal restrictions that the CKMS is intended to enforce

4.9 Security Domains

- Specify whether or not the CKMS is intended to allow exchange of keys and metadata with entities in other security domains
- Specify the confidentiality, integrity, and source authentication policies that are enforced when communicating with entities from other security domains

4.9 Security Domains (2)

- Specify what assurances are required when communicating with entities from other domains
- Specify requirements for reviewing and verifying the Security Policies of other domains
- Specify policies regarding third-party sharing
- Specify if multi-level security is provided and how it is maintained
- Specify conditions for up-grading and down-grading

5. Roles and Responsibilities

- System Authority, System Administrator, Cryptographic Officer, Domain Authority, Key Custodian, Key Owner, System User, Audit Administrator, Registration Agent, Key Recovery Agent, CKMS Operator

5. Roles and Responsibilities (2)

- Specify each role that the CKMS supports
- Specify key and metadata management functions (6.4) used by each role.
- Specify which roles require separation (e.g., System Administrator and Audit Administrator) and how it is maintained
- Specify automated provisions for identifying security violations

6. Cryptographic Keys and Metadata

- ★6.1 Key Types
- ★6.2 Key Metadata
- 6.3 Key Life Cycle States and Transitions
- ★6.4 Key and Metadata Management Functions
- 6.5 Key and/or Metadata Security: In Storage

Cryptographic Keys and Metadata (2)

- 6.6 Key and/or Metadata Security: During Key Establishment
- 6.7 Restricting Access to Key and Metadata Management Functions
- 6.8 Compromise Recovery

6.1 Key Types

1. Private Signature Key
2. Public Signature Key
3. Symmetric Authentication Key
4. Private Authentication Key
5. Public Authentication Key
6. Symmetric Data Enc/Dec Key
7. Symmetric Key Wrapping Key
8. Symmetric RNG Key
9. Private RNG Key
10. Public RNG Key
11. Symmetric Master Key
12. Private Key Transport Key
13. Public Key Transport Key
14. Symmetric Key Agreement Key
15. Private Static Key Agreement Key
16. Public Static Key Agreement Key
17. Private Ephemeral Key Agreement Key
18. Public Ephemeral Key Agreement Key
19. Symmetric Authorization Key
20. Private Authorization Key
21. Public Authorization Key

6.1 Key Types

- Specify and define each key type used

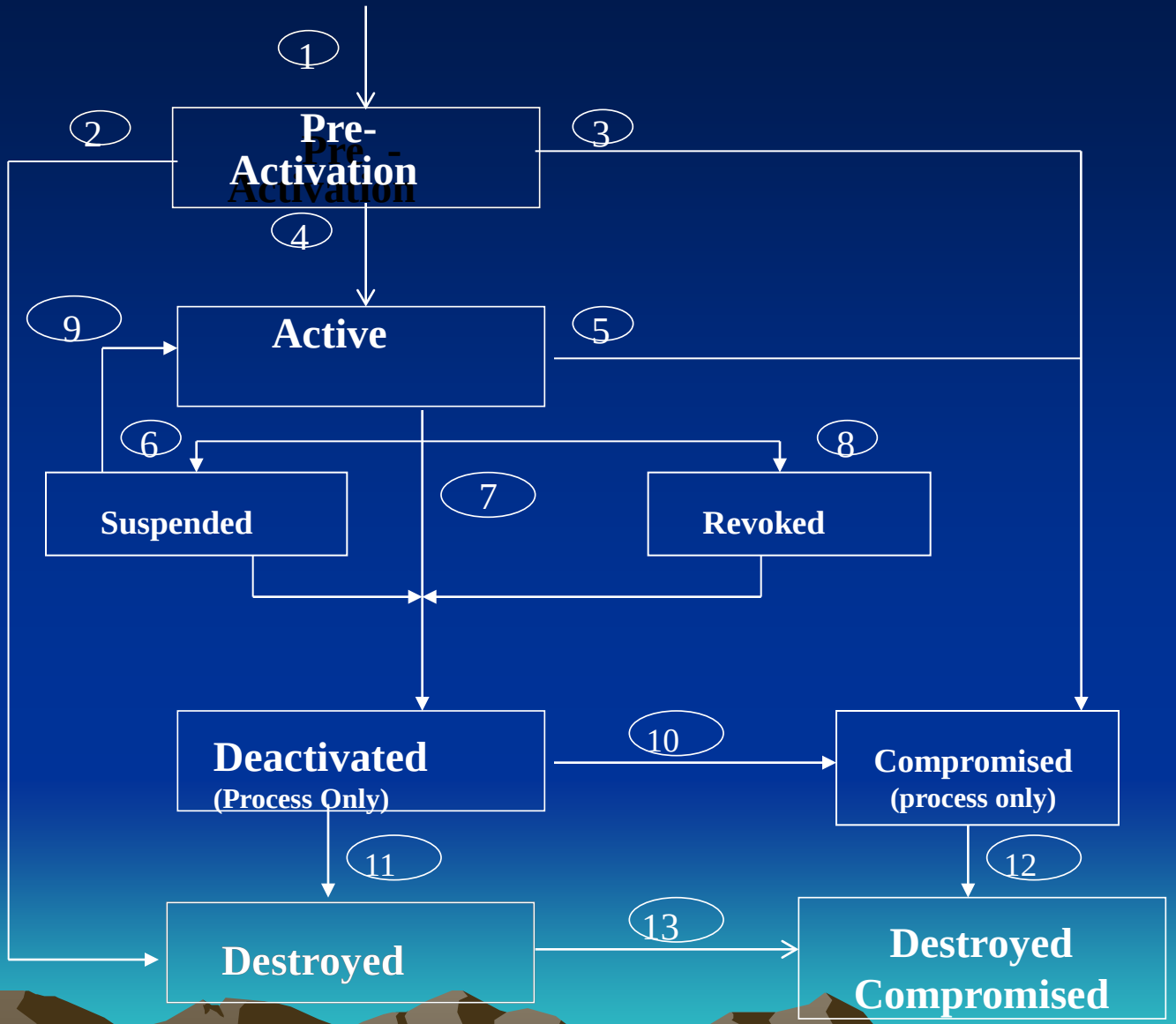
6.2 Key Metadata

1. Key Label
2. Key Identifier
3. Owner Identifier
4. Key Life Cycle State
5. Key Format Specifier
6. Product used to Create Key
7. Crypto Algorithm using key
8. Schemes or Modes of Operation
9. Parameters for the Key
10. Length of the Key
11. Strength of the Key-Algorithm Pair
12. Key Type
13. Applications for Key
14. Security Policies for Key
15. Key Access Control List
16. Key Usage Count
17. Parent Key
18. Key Sensitivity
19. Key Protections
20. Metadata Protection
21. Trusted Association Protection
22. Date-Times
23. Revocation Reason

6.2 Key Metadata (2)

- Specify which metadata elements are used in a trusted association with each CKMS key type
- Specify what protections are applied to keys and metadata (e.g., confidentiality, integrity, source of integrity authentication)
- Specify the processes used to enforce the trusted association
- Specify what authoritative time sources are used for dates and times

6.3 Key Life Cycle States and Transitions



6.3 Key Life Cycle States and Transitions

- Specify the CKMS cryptographic key states and transitions

6.4 Key and Metadata Management Functions

- The Framework lists 31 key and metadata management functions
  - Generation
  - Owner Registration
  - Activation
  - Deactivation
  - Etc.

6.4 Key and Metadata Management Functions

- Specify the key and metadata management functions to be implemented and supported
- Specify the integrity, confidentiality, and source authentication services that are applied to each key and metadata management function
- Specify the key generation methods used
- Specify the random number generators used
- Specify how and under what conditions can metadata be modified?
- Etc.

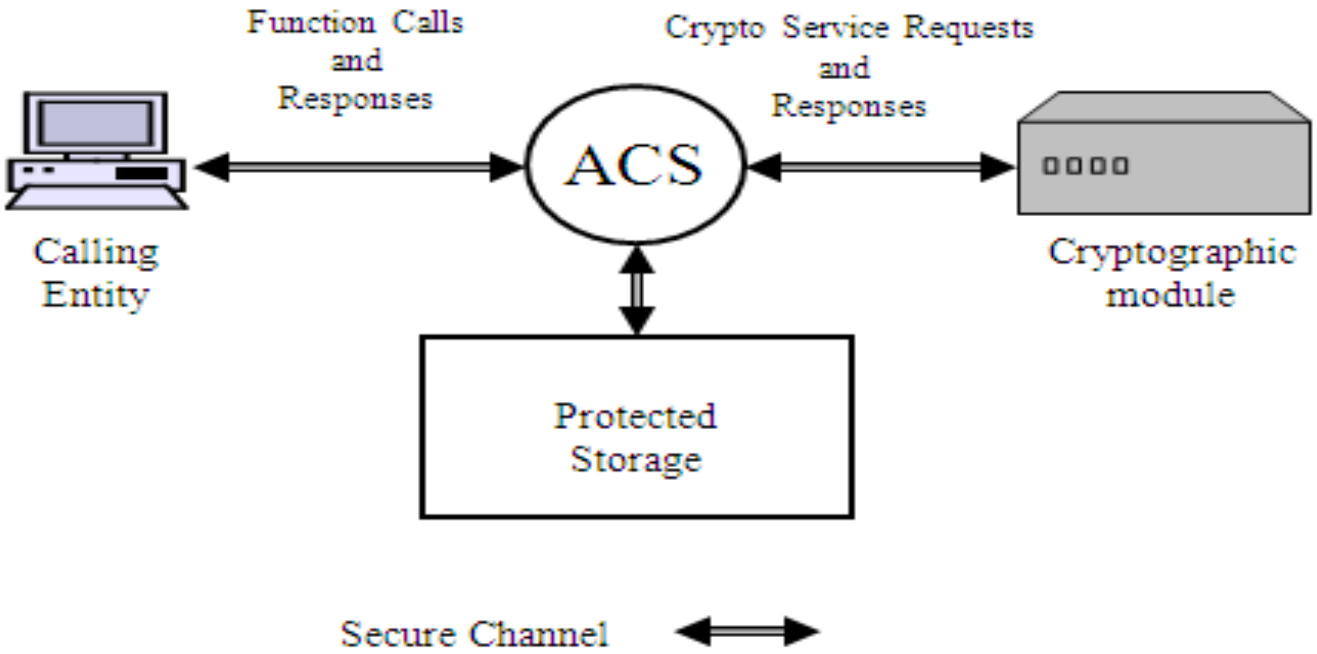
6.5 Cryptographic Key and/or Metadata: In Storage

- Specify how authorization for submitting, retrieving and using keys and metadata in storage verified
- Specify how the integrity and confidentiality of keys and metadata verified in storage
- If a KEK is used to protect stored keys, then specify the methods used to protect the KEK

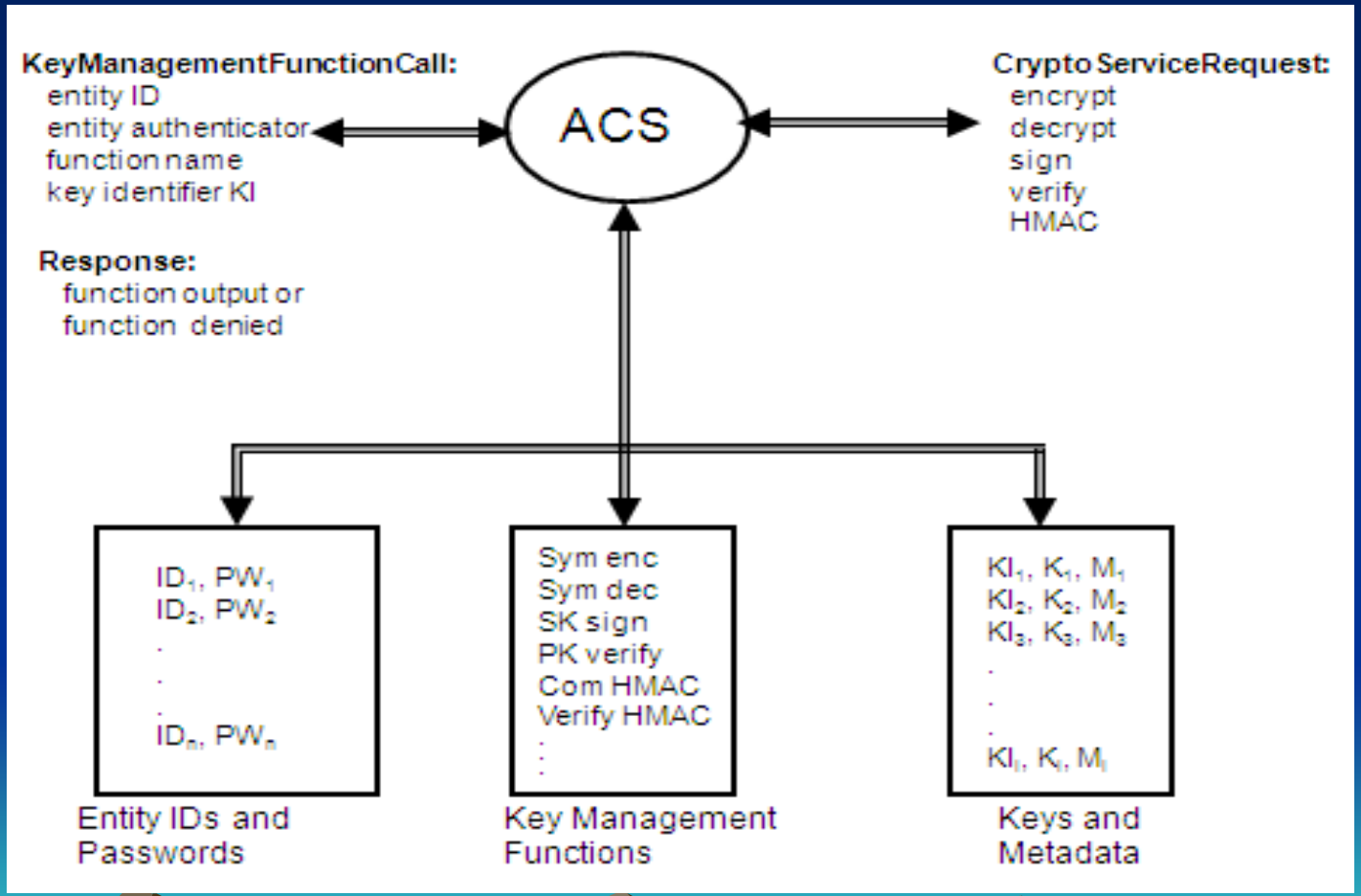
6.6 Cryptographic Key and Metadata Security: During Key Establishment

- Transport/Agreement
  - Specify what key establishment methods are used?
  - Specify how are keys protected during transport?
  - Specify how are the identifiers of the parties to key establishment assured?
  - Specify what key confirmation methods are used?
- Key Establishment Protocols
  - Specify all protocols that are used for key establishment and storage purposes

6.7 Restricting Access to Key and Metadata Management Functions



6.7 Restricting Access to Key and Metadata Management Functions



6.7 Restricting Access to Key and Metadata Management Functions

- Specify the topology of the CKMS by indicating the locations of the entities, the ACS, the function logic, and the connections between them
- Specify how access to key and metadata management functions is controlled (i.e., describe the ACS)
- Specify the capabilities of the ACS to support the security policy.

6.7 Restricting Access to Key and Metadata Management Functions (2)

- Specify conditions upon which plaintext secret or plaintext private keys are entered into or output from the CM
- Specify how plaintext secret or plaintext private keys are protected and controlled and audited
- Specify all human input parameters, their formats, and the action taken by the CKMS if they are not provided

6.7 Restricting Access to Key and Metadata Management Functions (3)

- Specify all functions that require multi-party control and/or key splitting.
- Specify (n, k) for each

6.8 Compromise Recovery

- Specify what are the cryptographic periods of the keys
- ★ Specify how are key compromises handled and what other keys are affected
- ★ Specify which metadata elements are sensitive to compromise, possible consequences, and remedies

6.8 Compromise Recovery (2)

- Specify the key revocation mechanism(s) and associated relying entity notification mechanism(s)

6.8 Compromise Recovery (3)

- Cryptographic Modules
  - Specify how access to the cryptographic module contents restricted
  - Specify the approach to recover from a CM compromise
  - Specify what non-invasive attacks are mitigated by the module
  - Specify modules that are vulnerable to non-invasive attacks and rationale for accepting the vulnerabilities

6.8 Compromise Recovery (4)

- Specify mechanisms used to detect unauthorized modifications to CKMS system HW, SW, and data.
- Specify how CKMS recovers from unauthorized modifications the CKMS system HW,SW, and data

6.8 Compromise Recovery (5)

- Specify compromise recovery responsibilities assigned to each role
- ★ Specify all automated CKMS recovery features for personnel security compromise

6.8 Compromise Recovery (6)

- Specify how components and devices are physically protected
- Specify how unauthorized physical access is detected
- Specify how CKMS recovers from unauthorized physical access
- Specify entities that are automatically notified
- Specify how breached areas are re-established

7. Interoperability and Transitioning

- Specify how interoperability requirements are to be satisfied
- Specify standards, protocols, interfaces and commands required to support interoperability
- Specify all external interfaces and upgrading provisions
- Specify protocols for negotiating cryptographic algorithms

8. Security Controls

8.1 Physical Security Controls

8.2 Operating System and Device Security Controls

8.3 Network Security Control Mechanisms

8.4 Cryptographic Module Controls

8.1 Physical Security Controls

- Specify each CKMS device and its intended purpose
- Specify the physical security controls for protecting each CKMS device
- What operating system requirements does the CKMS require?
- What system monitoring is performed?
- What are the requirements for anti-virus and anti-spyware protection?
- What types of firewalls and firewall configuration are required?

8.2 Operating System and Device Security Controls

- Specify operating system's secure configuration and hardening requirements for each CKMS device
- Specify security configuration and security controls for each CKMS device
- Specify the malware protection capabilities of each CKMS device
- Specify software integrity verification procedures

8.2 Operating System and Device Security Controls (2)

- Specify auditable events
- If configurable, specify roles that may configure the audit feature
- Specify data to be recorded
- What automated tools are provided to assess the correct operation of the CKMS
- Specify system monitoring requirements for sensitive system files

8.3 Network Security Control Mechanisms

- Specify boundary protection mechanisms employed by the CKMS
- Specify how the CKMS protects against denial of service

8.4 Cryptographic Module Controls

- Specify the CMs used and their respective security policies

9 Testing and System Assurances

9.1 Vendor Testing

9.2 Third-Party Testing

9.3 Interoperability Testing

9.4 Self-Testing

9.5 Scalability Testing

9.6 Functional Testing and Security Testing

9.7 Limitations of Testing

9.8 Development Assurance

9.1 Vendor Testing

- Specify the non-proprietary vendor testing that was performed on the CKMS and passed

9.2 Third-Party Testing

- Specify all third-party testing programs that have been passed to date

9.3 Interoperability Testing

- If the CKMS claims interoperability with another system, then specify the tests that have been performed and passed
- If the CKMS claims interoperability with another system, then specify any configuration settings that are required for interoperability

9.4 Self-Testing

- Specify all self-tests created (and implemented) by the designer and the corresponding CKMS functions that they verify

9.5 Scalability Testing

- Specify all scalability testing performed on the system to date

9.6 Functional Testing and Security Testing

- Specify the functional and security testing that was performed on the system and the results of the tests

9.7 Limitations of Testing

- Specify the environments in which the CKMS is to be used
- Specify the conditions that are required for its secure operation
- Specify the results of environmental testing that was performed

9.8 Development Assurance

- Specify all devices to be kept under configuration control
- Specify protection requirements to ensure that only authorized changes are made to the components and devices under control
- Specify secure delivery requirements for the products used in the CKMS

9.8 Development Assurance (2)

- Specify the security requirements for the development and maintenance environment used for CKMS product development
- Specify the CKMS capabilities for detecting, reporting, and analyzing system flaws
- Specify the CKMS capabilities for implementing fixes in a timely manner

10 Disaster Recovery

- 10.1 Facility Damage
- 10.2 Utility Service Outage
- 10.3 Communication and Computation Outage
- 10.4 System Hardware Failure
- 10.5 System Software Failure
- 10.6 Cryptographic Module Failure
- 10.7 Corruption of Keys and Metadata

10 Disaster Recovery (10.1-10.3)

- Specify the environmental, fire, and physical access control protection mechanisms and procedures for recovery from damage to primary and backup facilities
- Specify the minimum electrical, water, sanitary, heating, cooling, and air filtering requirements for the primary and backup facilities
- Specify the communications and computation redundancy present in the design to assure continued operation of services

10 Disaster Recovery (10.4-10.5)

- Specify the strategy for backup and recovery from failures of hardware components and devices
-  Specify all techniques used to verify the correctness of the system software, detect alterations in memory, and recover from a major software failure

10.6 Cryptographic Module Failure

- Specify what self-tests are used by each CM to detect errors and verify the integrity of the modules
- Specify how the CM responds to detected errors
- Specify the strategy for repair and replacement of failed CMs

10.7 Corruption of Keys and Metadata

- Specify procedures for restoring and replacing corrupted stored or transmitted keys and their metadata
- Specify procedures for backing-up and archiving cryptographic keys and their metadata

11 Security Assessment

11.1 Full Security Assessment

11.2 Periodic Security Review

11.3 Incremental Security Assessment

11.4 Security Maintenance

11.1 Full Security Assessment

- Specify assurance activities to be undertaken prior to or in conjunction with CKMS deployment?
- Specify the circumstances under which a full security assessment will be repeated
- Specify all validation programs and certificate numbers under which any of the CKMS devices have been validated
- Specify whether an architectural review is required. If so, specify the skill sent of the evaluation team.

11.1 Full Security Assessment (2)

- Specify all required functional and security testing of the CKMS and any results
- Specify specific areas where penetration testing has been performed and the results

11.2 Periodic Security Review

- Specify the periodicity of security reviews
- Specify the scope of the security review in terms of the CKMS devices
- Specify the scope of the security review in terms of the activities undertaken for each device under review
- Specify the functional and security testing to be performed as part of the periodic security review

11.3 Incremental Security Assessment

- Specify the circumstances under which and incremental security assessment will be conducted
- Specify the scope of the incremental security assessment

11.4 Security Maintenance

- List the maintenance activities required to maintain CKMS security

12. Technological Challenges

- Specify the expected security lifetime of each cryptographic algorithm used
- Specify which sub-routines of the cryptographic algorithms can be upgraded or replaced with similar, but cryptographically improved sub-routines
- Specify which key establishment protocols are used by the system
- Specify the security lifetime of each key establishment protocol used in the system

12 Technological Challenges

- Specify the extent to which external access to CKMS devices is permitted
- Specify how all allowed external accesses are controlled
- Specify the features employed to resist or mitigate the consequences of a quantum computing attack
- Specify the currently known consequences of a quantum computing attack on the CKMS

Final Thoughts

- A CKMS may involve all the security issues of the typical computer system (e.g., communications security, computer security, physical security, disaster recovery, etc.).
- However, a Framework could help classify, compare and standardize CKMS.
- Without a specification, a CKMS cannot be evaluated (for security or for practicality).
- Are we asking for to much?
- How can we simplify it?
- To obtain a copy of second public comment draft SP 800-130, see http://csrc.nist.gov/publications/PubsDrafts.html

Discussion?